PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2001-103045**
(43)Date of publication of application : **13.04.2001**

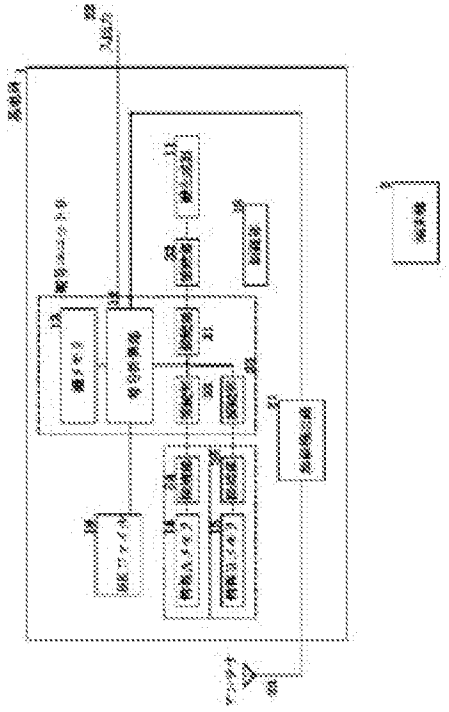
(51)Int.Cl. **H04L 9/08**
G06F 12/14
G06F 12/16
H04L 9/10

(21)Application number : **11-276798**
(22)Date of filing : **29.09.1999**

(71)Applicant : **ADVANCED MOBILE TELECOMMUNICATIONS SECURITY TECHNOLOGY RESEARCH LAB CO LTD**
(72)Inventor : **TSURUMARU JUNICHIRO**

(54) STORAGE DEVICE FOR BACKING UP CRYPTOGRAPHIC KEY

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent backup file of cryptographic keys from being physically decoded easily and also to recover cryptographic keys, even if a part of the cryptographic keys fails.
SOLUTION: A plurality of communication cryptographic keys used for communication are stored in a tamper-proof key memory 13. Secret information A and B are respectively stored in tamper-proof information A memory and information B memory 15, which are different from the memory 13. A cipher-calculating part 12 generates a cryptographic key for backup from the information A and B, enciphers a plurality of communication cryptographic keys and stores them in a backup file 18. In the case of recovery, the enciphered communication cryptographic keys are decoded with the cryptographic key for backup. Safety can be enhanced, because the communication cryptographic keys cannot be decoded unless obtaining the plurality of memory information and the backup file.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－103045
（P2001－103045A）
(43)公開日　平成13年４月13日(2001.4.13)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	12/16	３１０Ｍ	５Ｂ０１８
12/16	３１０	Ｈ０４Ｌ　9/00	６０１Ａ	５Ｊ１０４
Ｈ０４Ｌ　9/10			６２１Ａ	

審査請求　有　　請求項の数11　ＯＬ　（全 12 頁）

(21)出願番号　特願平11－276798

(22)出願日　平成11年９月29日(1999.9.29)

(71)出願人　597174182
株式会社高度移動通信セキュリティ技術研究所
神奈川県横浜市港北区新横浜三丁目20番地８

(72)発明者　鶴丸　純一郎
神奈川県横浜市港北区新横浜三丁目20番地８　株式会社高度移動通信セキュリティ技術研究所内

(74)代理人　100099254
弁理士　役　昌明　（外１名）

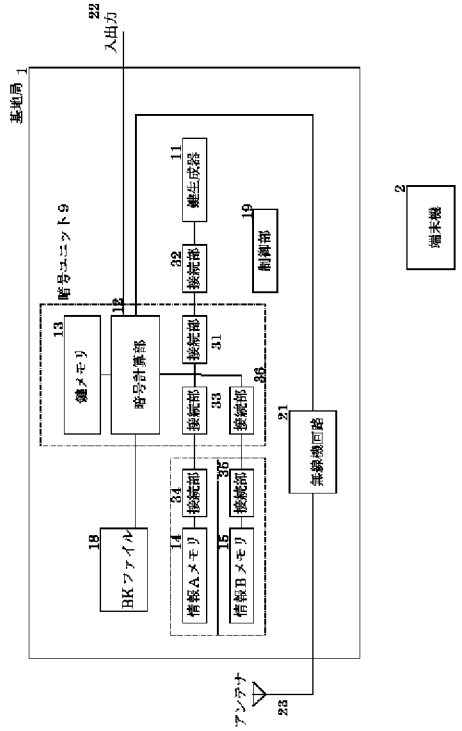
最終頁に続く

(54)【発明の名称】　暗号鍵バックアップ記憶装置

(57)【要約】

【課題】　暗号鍵のバックアップファイルを物理的に簡単には解読できないようにするとともに、一部が故障しても暗号鍵をリカバーできるようにする。

【解決手段】　通信に使う複数の通信暗号鍵を、耐タンパー性の鍵メモリ13に記憶する。秘密情報Ａ，Ｂを、それぞれ鍵メモリ13とは別の耐タンパー性の情報Ａメモリ14と情報Ｂメモリ15に記憶する。暗号計算部12で、秘密情報Ａ，Ｂからバックアップ用暗号鍵を生成して、複数の通信暗号鍵を暗号化してバックアップファイル18に格納する。リカバリーのときは、暗号化された通信暗号鍵をバックアップ用暗号鍵で復号する。複数のメモリの情報とバックアップファイルを入手しないと通信用暗号鍵を解読できないので、安全性を高めることができる。



【特許請求の範囲】

【請求項１】　暗号通信装置の暗号鍵バックアップ記憶装置において、通信に使う複数の通信暗号鍵を記憶する耐タンパー性の第１の記憶手段と、複数に分割した秘密情報をそれぞれ記憶する耐タンパー性の独立の複数の記憶手段からなる第２の記憶手段と、暗号計算手段と、バックアップファイル手段とを具備し、前記暗号計算手段は、前記複数の秘密情報に基づいてバックアップ用暗号鍵を生成する手段と、前記バックアップ用暗号鍵で前記複数の通信暗号鍵を暗号化して前記バックアップファイル手段に格納する手段と、暗号化された前記複数の通信暗号鍵を前記バックアップファイル手段から取り出して前記バックアップ用暗号鍵で復号して前記第１の記憶手段に格納する手段とを有することを特徴とする暗号鍵バックアップ記憶装置。

【請求項２】　前記バックアップ用暗号鍵をＫとし、十分に大きな素数をｐ，ｑ（ｐ≠ｑ）とし、十分に大きな整数をｎ（ｎ＞Ｋ）とし、$K^p \bmod n$をSaとし、$K^q \bmod n$をSbとして、前記第２の記憶手段の１つに第１の秘密情報として前記Sa，ｐ，ｎを記憶し、他の１つに第２の秘密情報として前記Sb，ｑ，ｎを記憶することを特徴とする請求項１に記載した暗号鍵バックアップ記憶装置。

【請求項３】　前記第２の記憶手段の１つに第１の秘密情報として公開鍵暗号の秘密鍵を記憶し、他の１つに第２の秘密情報として前記バックアップ用暗号鍵を公開鍵暗号の公開鍵で暗号化した数値を記憶することを特徴とする請求項１に記載した暗号鍵バックアップ記憶装置。

【請求項４】　前記第２の記憶手段の１つに第１の秘密情報として秘密鍵暗号の秘密鍵を記憶し、他の１つに第２の秘密情報として前記バックアップ用暗号鍵を秘密鍵暗号の秘密鍵で暗号化した数値を記憶することを特徴とする請求項１に記載した暗号鍵バックアップ記憶装置。

【請求項５】　暗号通信装置の暗号鍵バックアップ記憶装置において、通信に使う複数の通信暗号鍵を記憶する耐タンパー性の第１の記憶手段と、第１、第２、第３の秘密情報をそれぞれ記憶する耐タンパー性の独立の３つの記憶手段からなるである第２の記憶手段と、暗号計算手段と、バックアップファイル手段とを具備し、前記暗号計算手段は、前記第１の秘密情報と前記第２の秘密情報と前記第３の秘密情報の中の任意の２つの秘密情報に基づいてバックアップ用暗号鍵を生成する手段と、前記バックアップ用暗号鍵で前記複数の通信暗号鍵を暗号化して前記バックアップファイル手段に格納する手段と、暗号化された前記複数の通信暗号鍵を前記バックアップファイル手段から取り出して前記バックアップ用暗号鍵で復号して前記第１の記憶手段に格納する手段とを有することを特徴とする暗号鍵バックアップ記憶装置。

【請求項６】　前記バックアップ用暗号鍵をＫとし、十分に大きな素数をｐ，ｑ，ｒ（ｐ≠ｑ≠ｒ≠ｐ）とし、十分に大きな整数をｎ（ｎ＞Ｋ）とし、$K^p \bmod n$をSaとし、$K^q \bmod n$をSbとし、$K^r \bmod n$をScとして、前記第２の記憶手段の１つに前記第１の秘密情報として前記Sa，ｐ，ｎを記憶し、他の１つに前記第２の秘密情報として前記Sb，ｑ，ｎを記憶し、さらに他の１つに前記第３の秘密情報として前記Sc，ｒ，ｎを記憶することを特徴とする請求項５に記載した暗号鍵バックアップ記憶装置。

【請求項７】　暗号通信装置の暗号鍵バックアップ記憶装置において、通信に使う複数の通信暗号鍵を記憶する耐タンパー性の第１の記憶手段と、ｍ個（ｍ＞３）の秘密情報をそれぞれ記憶する耐タンパー性の独立のｍ個の記憶手段からなる第２の記憶手段と、暗号計算手段と、バックアップファイル手段とを具備し、前記暗号計算手段は、前記ｍ個の秘密情報の中の任意のｔ個（１＜ｔ＜ｍ）の秘密情報に基づいてバックアップ用暗号鍵を生成する手段と、前記バックアップ用暗号鍵で前記複数の通信暗号鍵を暗号化して前記バックアップファイル手段に格納する手段と、暗号化された前記複数の通信暗号鍵を前記バックアップファイル手段から取り出して前記バックアップ用暗号鍵で復号して前記第１の記憶手段に格納する手段とを有することを特徴とする暗号鍵バックアップ記憶装置。

【請求項８】　前記第２の記憶手段のそれぞれをモジュール単位で交換できる１つのモジュールとして構成したことを特徴とする請求項１、５、７のいずれかに記載した暗号鍵バックアップ記憶装置。

【請求項９】　前記第１の記憶手段と前記暗号計算手段を一体に構成した第１のモジュールと、前記第１のモジュールと前記第２の記憶手段との間を中継接続する耐タンパー性の第２のモジュールとを設けたことを特徴とする請求項８に記載した暗号鍵バックアップ記憶装置。

【請求項１０】　前記第２の記憶手段と前記第２のモジュールとが接続か非接続かを検出する手段と、前記第２の記憶手段のモジュールと前記第２のモジュールとが非接続となったことを検出したときに前記第２の記憶手段の記憶内容を消去する手段とを有することを特徴とする請求項９に記載した暗号鍵バックアップ記憶装置。

【請求項１１】　前記第２の記憶手段の中の一部の記憶手段を離れた場所に設置して伝送路を介して接続したことを特徴とする請求項１、５、７のいずれかに記載した暗号鍵バックアップ記憶装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号鍵バックアップ記憶装置に関し、特に、暗号通信装置に記憶している暗号鍵を、故障に備えたバックアップファイルに安全にバックアップしたりリカバーする暗号鍵バックアップ記憶装置に関する。

【０００２】

【従来の技術】端末機の数が多く、多数の暗号鍵を使用

する従来の通信システムでは、暗号化のため暗号鍵（通信用暗号鍵）を多数使用する。大きな通信システムで、端末機個別に暗号鍵を割り当てるようなシステムでは、基地局装置の中に多数の暗号鍵を保管して使用する。例えば、10万台の端末機を使用し、10万個の暗号鍵を使用することもある。このように多数の暗号鍵を使用するシステムでは、暗号鍵を常駐メモリに記憶しておくとともに、故障に備えて定期的に暗号鍵のバックアップファイルをとっておく。機械が故障し、メモリに書いてあった暗号鍵が消えたしまったときは、バックアップファイルより記憶装置に入れ直す。

【０００３】現代暗号を利用した通信システムでは、暗号アルゴリズムは公開されていても、暗号鍵を秘密にしておけば、情報の秘密を守ることができることを原理としている。設計者やメンテナンス技術者は、暗号アルゴリズムを知っているのが当然であるが、暗号鍵を知らなければ、設計者であっても、メンテナンス技術者であっても、情報の秘密を解読できない。したがって、バックアップファイルを含めて、暗号鍵を秘密にする必要がある。秘密にするには、暗号鍵を更に暗号化して、バックアップファイルに記憶する。

【０００４】ところが、故障対策のため持ち運び可能な記憶媒体に暗号鍵のバックアップファイルを取ると、使用場所から外部へ持ち出すことができるので、暗号方式によっては関係者がバックアップファイルの暗号鍵を盗み出すことが可能になる。大きなシステムでは、従業員や保守会社の技術者など多くの人が、運用保守に関係するので、このような人が、故意にまたは不注意で秘密を漏らすことがないように、関係者の倫理性や人事管理に依存した厳重な秘密管理をしている。

【０００５】

【発明が解決しようとする課題】しかし、上記従来の装置では、バックアップに使う暗号鍵の秘密を、関係者が故意にまたは不注意で漏らすことが絶対にないとは言い切れないので、関係者の倫理性や人事管理だけに頼って秘密を保持することには限界があるという問題があった。第三者のみならず関係者に対しても、暗号鍵の秘密の保持を必要とする。

【０００６】また、バックアップファイルが故障すると暗号鍵をリカバーできなくなるという問題もあった。信頼性の点からは、１個の部品が故障しても暗号鍵のリカバリーに支障がないという装置にすることが望ましい。

【０００７】本発明は、上記従来の問題を解決して、第三者のみならず保守や運用に当たる人でも、暗号鍵のバックアップファイルを物理的に簡単には解読できないようにして、暗号鍵に関する秘密情報を入手することを困難にすることを目的とする。また、バックアップファイルの一部が故障してもリカバーできるようにすることも目的とする。

【０００８】

【課題を解決するための手段】上記の課題を解決するために、本発明では、暗号通信装置の暗号鍵バックアップ記憶装置を、通信に使う複数の通信暗号鍵を記憶する耐タンパー性の第１の記憶手段と、複数に分割した秘密情報をそれぞれ記憶する耐タンパー性の独立の複数の記憶手段からなる第２の記憶手段と、暗号計算手段と、バックアップファイル手段とを具備し、暗号計算手段は、複数の秘密情報に基づいてバックアップ用暗号鍵を生成する手段と、バックアップ用暗号鍵で複数の通信暗号鍵を暗号化してバックアップファイル手段に格納する手段と、暗号化された複数の通信暗号鍵をバックアップファイル手段から取り出してバックアップ用暗号鍵で復号して第１の記憶手段に格納する手段とを有する構成とした。

【０００９】このように構成したことにより、独立の部品である複数の記憶手段からの秘密情報とバックアップファイルを入手しないと暗号鍵を解読できなくなり、第三者のみならず従業員などの関係者にも暗号鍵の入手が困難になって、バックアップ／リカバリー過程における安全性を高めることができる。

【００１０】また、暗号通信装置の暗号鍵バックアップ記憶装置を、通信に使う複数の通信暗号鍵を記憶する耐タンパー性の第１の記憶手段と、第１、第２、第３の秘密情報をそれぞれ記憶する耐タンパー性の独立の３つの記憶手段からなるである第２の記憶手段と、暗号計算手段と、バックアップファイル手段とを具備し、暗号計算手段は、第１の秘密情報と第２の秘密情報と第３の秘密情報の中の任意の２つの秘密情報に基づいてバックアップ用暗号鍵を生成する手段と、バックアップ用暗号鍵で複数の通信暗号鍵を暗号化してバックアップファイル手段に格納する手段と、暗号化された複数の通信暗号鍵をバックアップファイル手段から取り出してバックアップ用暗号鍵で復号して第１の記憶手段に格納する手段とを有する構成とした。

【００１１】このように構成したことにより、３つの秘密情報を記憶する記憶手段の１つが故障しても、２つの記憶手段の秘密情報からバックアップ用暗号鍵を生成してバックアップ／リカバリーができ、耐故障性が向上する。

【００１２】

【発明の実施の形態】以下、本発明の実施の形態について、図１～図４を参照しながら詳細に説明する。

【００１３】（第１の実施の形態）本発明の第１の実施の形態は、秘密情報Ａを耐タンパー性の独立の情報Ａメモリに記憶し、秘密情報Ｂを耐タンパー性の独立の情報Ｂメモリに記憶し、秘密情報ＡとＢから生成したバックアップ用暗号鍵で通信暗号鍵を暗号化してバックアップファイルに格納し、暗号化された通信暗号鍵をバックアップ用暗号鍵で復号してリカバーする暗号鍵バックアップ記憶装置である。

【００１４】図１は、本発明の第１の実施の形態における暗号鍵バックアップ記憶装置を備えた無線通信システムの機能ブロック図である。図１において、基地局１は、無線の基地局である。端末機２は、無線の端末機（移動機）である。端末機２は、複数台存在している。基地局１は、通常の無線機の機能としての無線機回路21、入出力部22、アンテナ23に加えて、鍵生成器11、暗号計算部12、鍵メモリ13、情報Ａメモリ14、情報Ｂメモリ15、ＢＫファイル18、制御部19、部分ユニット化を行うときの接続部31、32、33、34、35、36などの機能ユニット（電子回路）で構成されている。

【００１５】１．上記のように構成された、本発明の第１の実施の形態における暗号鍵バックアップ記憶装置の各部の機能を説明する。鍵生成器11は、基地局１の装置の外からは知ることができない状態で暗号鍵や後述する秘密情報を生成し、ディジタル信号として、暗号計算部12や端末機２などへ供給するものである。通信に使う暗号鍵は、当然、基地局装置と端末機で同じ暗号鍵を保有するので、端末機２へも暗号鍵を供給することになる。

【００１６】どのようにして装置の外からは知ることができない状態で暗号鍵を生成するかは、本発明の対象外であるが、一例として、熱雑音がランダムに発生することを原理とした乱数発生器で乱数を発生し、その乱数から暗号鍵として適当な数を選択したり、乱数を演算して暗号鍵を求める方法がある。多数の乱数を発生させ、その中から素数を取り出すとか、素数を２つ生成し、その積を求めるなどの鍵生成機能を持つ。端末機２への暗号鍵の供給方法も、本発明の対象外であるが、端末機への暗号鍵の配信過程から暗号鍵に関する情報が漏れないものとする。暗号鍵の基地局１内の配信過程で暗号鍵の秘密情報が盗まれるかどうかの問題も本発明の対象外であるが、生成した暗号鍵が生成と配信過程で盗まれない条件付きで暗号鍵を生成／配信するものとする。

【００１７】暗号計算部12は、端末機２へ送信する平文のアプリケーション情報を鍵メモリ13に記憶している通信暗号鍵（以下、アプリケーション情報の暗号化／復号に使う暗号鍵を通信暗号鍵と呼ぶ）を用いて暗号文へ暗号化する。端末機２から受信した暗号文のアプリケーション情報を鍵メモリ13に記憶している通信暗号鍵を用いて平文に復号する。鍵メモリ13に記憶している通信暗号鍵をバックアップファイルへバックアップするときに、鍵メモリ13に記憶している通信暗号鍵を暗号化する。鍵メモリ13に記憶させる通信暗号鍵をバックアップファイルからリカバーするときに、鍵メモリ13に記憶させるために通信暗号鍵を復号する。さらには、情報Ａメモリ14、情報Ｂメモリ15に記憶させる秘密情報を生成し、情報Ａメモリ14、情報Ｂメモリ15へ送り記憶させる。通常は、暗号計算部12をマイクロコンピュータにより構成する。

【００１８】鍵メモリ13は、多数の通信暗号鍵を記憶する記憶素子である。通常は、端末機ごとに異なる複数の通信暗号鍵を、鍵生成器11より暗号計算部12経由で受け取って、そのまま記憶しておき、通信の暗号化／復号に使用するときに、暗号計算部12へ供給する。鍵メモリ13は、情報Ａメモリ14、情報Ｂメモリ15とは別のモジュール（取り替え修理が独立にできる）にする。鍵メモリ13の記憶内容は、電気的にそのまま暗号計算部12以外へ出すことはなく、必ず暗号計算部12で暗号化されて暗号計算部12以外へ出すものとする。すなわち、通信暗号鍵を電気的に外部へ出力する（取り出す）ときは、暗号計算部12によって必ず暗号文になる仕組みになっている。鍵メモリ13では、通信暗号鍵を記憶するに当たり、暗号化する必要がない。鍵メモリ13に記憶されている暗号鍵は、誰にも知られないようにするものとする。そのため、記憶中の暗号鍵を読み出す（盗み出す）ことを防止するため、このメモリは、耐タンパー性能（内部構造を調べることにより記憶内容を調べることが困難な性能）に優れたものにする。鍵メモリ13に使うメモリ素子は、故障したらバックアップファイルからリカバーするので、電源が切れたら記憶内容が消えるＤＲＡＭでもよいし、むしろその方が耐タンパー性の点から望ましい。

【００１９】情報Ａメモリ14、情報Ｂメモリ15は、バックアップに使うＢＫ暗号鍵を生成する秘密の情報（１つの情報は複数のパラメータからなっていることがある）を、１組または多くても数組程度記憶する記憶素子である。暗号計算部12より秘密情報を受け取って記憶しておき、バックアップファイルへバックアップするときとリカバーするときに、秘密情報を暗号計算部12へ供給する。情報Ａメモリ14、情報Ｂメモリ15に記憶する秘密情報は、それぞれのメモリに記憶する情報だけではＢＫ暗号鍵を求めるのが計算量的に不可能であるが、情報Ａメモリ14、情報Ｂメモリ15両方のメモリに記憶する秘密情報を両方とも入手すると、ＢＫ暗号鍵を求めることができる性格のものである。

【００２０】情報Ａメモリ14、情報Ｂメモリ15から暗号計算部12へ秘密情報を供給するパス（電気回路）は、装置の内部回路とし、装置の外から盗聴することが困難なパスにする。バックアップ鍵を生成するための秘密情報は、情報Ａメモリ14、情報Ｂメモリ15から、直接暗号計算部12へ渡すもので、その他の部分へこの秘密情報が渡される（電気的に転送される）ことはない。すなわち、装置の他の部分から電気的に情報Ａメモリ14および情報Ｂメモリ15へアクセスすることはできない。

【００２１】情報Ａメモリ14および情報Ｂメモリ15は、それぞれが鍵メモリ13とは別のモジュール（取り替え修理が独立にできる）にする。このメモリは、耐タンパー性能に優れたものにした方がよい。反面、情報Ａメモリ14、情報Ｂメモリ15に使うメモリ素子は、記憶する情報量が少なく、故障に備えてバックアップすることを考えなくてよいので、電気的に書き換え可能で、かつ電源が

切れても記憶内容が消えないファラッシュメモリなど電気的に書き換え可能なリードオンリーメモリを使う方が望ましい。また、後述するように、故障修理のことを考えると、情報Ａメモリ14、情報Ｂメモリ15は、プラグインできるもの（ＬＳＩを半田付けではなくソケットに挿入で電気的接続を行う形式）にしてもよい。

【００２２】ＢＫファイル18は、通信暗号鍵のバックアップ情報を記憶する装置（機器）である。通常は、記憶媒体を取り外して、持ち歩きできるフロッピー（登録商標）ディスク装置や光磁気ディスク装置などの外部記憶装置が使われる。暗号計算部12は、情報Ａメモリ14、情報Ｂメモリ15の秘密情報から、ＢＫ暗号鍵を生成する。さらに、このＢＫ暗号鍵で、鍵メモリ13に記憶している通信暗号鍵総てを暗号化して出力し、ＢＫファイル18へ格納する。また、ＢＫファイル18から入力したバックアップ情報を、ＢＫ暗号鍵を使って復号し、鍵メモリ13に格納することで、以前にバックアップしたものをリカバーする。ＢＫファイル18の媒体に記憶される通信暗号鍵は、ＢＫ暗号鍵で暗号化されているので、ＢＫ暗号鍵を知らないかぎり、解読できない。

【００２３】制御部19は、基地局の装置全体を、以下のように制御するものである。

（１）鍵生成器11に指令を出して、新しい暗号鍵を生成させ、端末機番号を新たに付与し、端末機２と暗号計算部12へ端末機番号と新しい通信暗号鍵を分配させる。

（２）暗号計算部12へ端末機番号を送り、その端末機の持つ通信暗号鍵を鍵メモリ13から選択せしめて、入出力部22より入力されるアプリケーション情報を、端末機番号をもとに選択した通信暗号鍵で暗号化して、無線機回路21へ送り、無線機回路21より受けた入力されるアプリケーション情報を、端末機番号をもとに選択した通信暗号鍵で復号して、入出力部22へ出力する。

（３）鍵メモリ13の記憶内容のバックアップ開始やリカバー開始を指示する。

（４）暗号計算部12に指令を送り、秘密情報を生成して、情報Ａメモリ14、情報Ｂメモリ15に記憶させる。

【００２４】無線機回路21は、一般的なディジタル無線機の回路である。送信に当たっては、ディジタル信号を高周波信号に変換して、アンテナへ送出する。受信に当たっては、アンテナから受信した高周波信号をディジタル信号に変換する。アンテナ23は、電波を送信したり、電波を受信するものである。

【００２５】入出力部22は、送受信するアプリケーション情報を入出力するものである。情報の種類としては、音声、文字、画像／映像などがあるが、本実施の形態では、いずれもディジタル信号として入出力されるものとする。

【００２６】基地局１の保全／修理を円滑に行うために、部分的にプラグイン交換ができるようにユニット化してもよい。この場合、暗号計算部12と鍵メモリ13を１つのユニットにする。それが、暗号ユニット９である。具体的な方法は本発明の対象ではないが、暗号ユニット９は、耐タンパー性に作るものとし、暗号ユニット９から通信暗号鍵の秘密が漏れないものとする。また、情報Ａメモリ14および情報Ｂメモリ15も、それぞれ耐タンパー性を持った１つのユニットにしてもよい。接続部31、接続部32、接続部33、接続部34、接続部35、接続部36は、ユニット化したユニットを他と電気的に接続するものであり、コネクターで接続する。

【００２７】２．情報Ａメモリ14、情報Ｂメモリ15に記憶する秘密情報の１例を説明する。情報Ａメモリ14に記憶する秘密情報をX1、情報Ｂメモリ15に記憶する情報をX2と命名する。X1は、Sa、ｐ、ｎの３つのパラメータで構成する。X2は、Sb、ｑ、ｎの３つのパラメータで構成する。ここで、ｐ、ｑは、ｐ≠ｑなる十分に大きな素数とする。ｎは、十分に大きな整数で、１つの秘密情報から暗号鍵を逆算することが困難な整数とする。逆算することが困難な整数とは、十分に大きな素数、十分に大きな２つ以上の素数の積などがある。

【００２８】Sa、Sbは、

$Sa = K^{p} \bmod n$

$Sb = K^{q} \bmod n$

により計算される数値である。ここで、Kは、ＢＫ暗号鍵とする。式は、整数Ｋをｐ乗したもの（ｐは整数）を整数ｎで割ったものの余りがSa（Saも整数）であることを意味する。（整数論の表現では、Saすなわち$K^{p} \bmod n$は、法ｎに関するK^{p}の剰余）整数ｎは、どちらか一方に記憶されていればよいが、記憶内容に対称性があった方が便利なことがあるため、両方に記憶するものとして説明する。なお、64ビット暗号鍵の場合、65ビット目を１にした数をKの代わりとして用いるとか、乱数を追加して512ビットの数字にして用いるなど、暗号鍵そのものではなく、一部、暗号鍵に変更を加えたものを秘密情報として使うケースもある。

【００２９】十分に大きな素数、整数とは、ＲＳＡ暗号の安全性の根拠と同じように、Sa、ｐ、ｎを知っても、Ｋを求めることが計算量的に困難な程度に大きな素数、整数ということである。なお、ＲＳＡ暗号とは異なり、フェルマーの小定理を原理としていないので、整数ｎは、必ずしも、２つの素数の積である必要がない。ただ、２つの素数の積にしておくと、ＲＳＡ暗号などの使用実績から、実用性を考えたときには、安全なｎの桁数などが定めやすい。

【００３０】秘密情報の生成・記憶方法としては、鍵生成器11で素数ｐ、ｑ、整数ｎ（例えば２素数の積）、暗号鍵Ｋ（Ｋ＜ｎ）を生成し、暗号計算部12でSa、Sbを計算して、秘密情報として情報Ａメモリ14、情報Ｂメモリ15に記憶させることができる。逆に秘密情報から暗号鍵Kを求めるときは、暗号計算部12は、情報Ａメモリ14、情報Ｂメモリ15から、Sa、Sb、ｐ、ｑ、ｎを入手し、計

算して暗号鍵Ｋを求めることができる。

【００３１】具体的には、整数ｐ、ｑが互いに素であるとき、すなわち、ｐ、ｑの最大公約数が１になるとき、

ａ×ｐ＋ｂ×ｑ＝１

となる整数ａ、ｂが存在する。このとき、必ず整数ａ、ｂの一方がプラスで、他方がマイナスになる。整数ａ、ｂが存在するときは、ｐ、ｑを数値として与えたとき、整数ａ、ｂの１組を求めることができる（例えば、池野信一、小山謙二著「現代暗号理論」電子情報通信学会発行、第17、18頁を参照）。

【００３２】今、ｂが負であったとすると、（ａが負のときは、以下の論議でａ、ｂを入れ替えて論議すればよい）

ａ×ｐ＝１－ｂ×ｑ

$K^{ap}=K^{1-bq}=K\times K^{-bq}$

$K^{ap} \bmod n=[K\times K^{-bq}] \bmod n$

ここで、先に定義し、計算してある

$Sa=K^{p} \bmod n$

$Sb=K^{q} \bmod n$

を代入すると、

$Sa^{a} \bmod n=[K\times Sb^{-b}] \bmod n$

となる。この式からＫを求めることは、合同式を解く問題であり、計算でＫを求めることができる（例えば、池野信一、小山謙二著「現代暗号理論」電子情報通信学会発行、第18～19頁を参照）。

【００３３】３．情報Ａメモリ14、情報Ｂメモリ15に記憶する秘密情報の別の例を説明する。X1は、ｄ、ｎの２つのパラメータで構成する。X2は、Ｃというパラメータで構成する。ｄはＲＳＡ暗号の秘密鍵、ｎはＲＳＡ暗号の公開鍵、ＣはＲＳＡ暗号の暗号文である。秘密情報を生成するときは、暗号計算部12は、暗号鍵生成器11から、ＲＳＡ暗号の公開鍵ｅ、ｎ、秘密鍵ｄとＢＫ暗号鍵Ｋを受け取る。続いて、暗号計算部12は、

$C=K^{e} \bmod n$

を計算し、ｄ、ｎを情報Ａメモリ14へ、Ｃを情報Ｂメモリ15へ記憶させる。秘密情報からＢＫ暗号鍵を求めるときは、情報Ａメモリ14と情報Ｂメモリ15を取り出し、

$K=C^{d} \bmod n$

を計算してＫを求める。この方法では、ｄ、ｎ、Ｃの３つの数値を知らないと、ＢＫ暗号鍵Ｋを求めることができない。なお、この方法は、情報Ａメモリ14、情報Ｂメモリ15に記憶する情報の形式が異なることになる。

【００３４】公開鍵暗号方式には多くの方式があるので、この考え方を拡張すると、一般論として、公開鍵暗号方式の暗号文と秘密鍵を情報Ａメモリ14と情報Ｂメモリ15に分けて記憶する方法が適用できる。また、公開鍵暗号方式に限定せずに秘密鍵暗号方式も利用できるので、秘密鍵暗号方式（例えばＤＥＳ暗号）の暗号文と秘密鍵を情報Ａメモリ14と情報Ｂメモリ15に分けて記憶する方法が適用できる。

【００３５】４．本発明の第１の実施の形態における暗号鍵の生成と記憶の動作を説明する。基地局１の使用前には、鍵メモリ13には、通信暗号鍵を何も書いていない。端末機に通信暗号鍵を書き込むときは、制御部19は、鍵生成器11に指令を送り、暗号鍵を生成させ、端末機２へ送らせるとともに、暗号計算部12を経由して、そのまま（暗号化しないで）鍵メモリ13へ書き込ませる。このとき、通信暗号鍵に合わせて、端末機の番号（正確には、端末機のハードウエアを識別する番号ではなく、アプリケーション情報の暗号化／復号に使う通信暗号鍵を識別する情報である）を鍵メモリ13に書き込ませる。どの端末機が、どの通信暗号鍵を使用するのか分かるようにするためである。登録する端末機２の台数が増えるに従って、鍵メモリ13に記憶する通信暗号鍵の数は増えていく。

【００３６】５．アプリケーション情報の送受信の動作を説明する。アプリケーション情報の送受信を行うときは、制御部19は、端末機番号を暗号計算部12に与える。暗号計算部12は、以降、制御部19が指定する端末機番号が変わるまで、その端末機番号に対応した通信暗号鍵を鍵メモリ13から取り出し、入出力部22から入力するアプリケーション情報を取り出した通信暗号鍵で暗号化して、無線機回路21へ送り出したり、無線機回路21から受信したアプリケーション情報を取り出した通信暗号鍵で復号して、入出力部22へ出力する。

【００３７】６．暗号鍵のファイルバックアップの動作を説明する。通信暗号鍵のバックアップファイルの作成を開始するときは、自動的かオペレーターの操作で、制御部19よりバックアップ開始の指示が出る。暗号計算部12は、鍵生成器11へ要求を出し、新しい暗号鍵１個をＢＫ暗号鍵として受け取り、先に詳述した計算方法で計算して秘密情報を生成して、情報Ａメモリ14と情報Ｂメモリ15に書き込ませる。この過程で、必要とするパラメータ（例えば、前記ｐ、ｑ、ｎ）は、鍵生成器11へ要求を出し、鍵生成器11から受け取る。書き込みを終わったら、暗号計算部12は、暗号鍵生成器11から受け取った情報を消去する。

【００３８】次に、暗号計算部12は、情報Ａメモリ14と情報Ｂメモリ15にある秘密情報を読み出し、先に詳述した計算方法で計算してＢＫ暗号鍵を求める。さらに、暗号計算部12は、鍵メモリ13に記憶している通信暗号鍵（多数個）を、順次、計算で求めたＢＫ暗号鍵で暗号化して、ＢＫファイル18に書き込む。総てのバックアップ情報をＢＫファイル18に書き込み終わるとバックアップが終了する。総てのバックアップ情報を送出した暗号計算部12は、不要になったＢＫ暗号鍵を廃棄する（メモリから消去する）。オペレーターは、ＢＫファイル18から記憶媒体を外し、安全なところに保管することができる。

【００３９】なお、情報Ａメモリ14と情報Ｂメモリ15に

記憶する秘密情報は、バックアップを行う都度生成して変更する方法と、一度生成すると、当分の間変更しない方法がある。変更しないときは、秘密情報の作成記憶過程を省略することになる。

【００４０】また、情報Ａメモリ14と情報Ｂメモリ15に３組（一般論としては複数組）の秘密情報を記憶できるようにし、バックアップを行う都度秘密情報を生成して変更するが、最新の３組（一般論としては複数組）の秘密情報のみを情報Ａメモリ14と情報Ｂメモリ15のメモリに残す方法もある。

【００４１】７．暗号鍵のリカバリー動作を説明する。リカバリーを開始するときは、オペレーターは、バックアップ情報を記憶している記憶媒体をＢＫファイル18にセットする。オペレーターのリカバリー開始の操作で、制御部19より暗号計算部12へリカバリー開始の指示が出る。暗号計算部12は、情報Ａメモリ14と情報Ｂメモリ15にある秘密情報を読み出し、先に詳述した計算方法で計算してＢＫ暗号鍵を求める。続いて、暗号計算部12は、順次、暗号化されているバックアップ情報をＢＫファイル18から読み出し、先に計算で求めたＢＫ暗号鍵で復号し、鍵メモリ13に通信暗号鍵（多数個）として書き込む。総てのバックアップされた情報を鍵メモリ13に書き込むとリカバリーを終了する。総てのバックアップされた情報をリカバーし終えた暗号計算部12は、不要になったＢＫ暗号鍵と計算に使った秘密情報を廃棄する。（メモリから消去する。）

８．安全性に関して説明する。バックアップファイルの媒体に記憶している通信暗号鍵を入手するためには、

（１）取り外し可能なバックアップファイルの媒体を入手して、その内容を読み出す。

（２）秘密情報を記憶するメモリを２個とも入手して、耐タンパー性になっているメモリの内容を読み出す。

（３）知っているアルゴリズムの知識を生かして、入手した情報を解析し解読する。

の３条件を必要とする。

【００４２】ところが、稼働中の機器から、情報Ａメモリ14と情報Ｂメモリ15の両方を取り外して入手することは、一般的に困難である。入手できたとしても、耐タンパー性にできている情報Ａメモリ14と情報Ｂメモリ15から、記憶内容を入手することは困難である。

【００４３】９．ユニット化とその効用について説明する。暗号計算部12と鍵メモリ13を一体化し、１つのユニット（暗号ユニット９）として、耐タンパー容器に収めてもよい。このようなユニットを用いれば、ユニットが故障したときは、暗号ユニット９全体を新しいユニットと一括交換し、新しいユニットへ、通信暗号鍵の情報をバックアップファイルからリカバーすることで、修理を行うことができる。交換したユニットは元々耐タンパー性があり、秘密が漏れる心配はないが、念のため、焼却処分のように完全に滅却するようにすればよい。

【００４４】なお、故障規模が大きく、基地局１の装置全体を交換する必要が生ずることがある。このようなときは、古い基地局１に内蔵されている情報Ａメモリ14と情報Ｂメモリ15を交換した新しい基地局１へ移動（持ち運び）しないかぎりバックアップファイルからのリカバリーができないという問題がある。情報Ａメモリ14と情報Ｂメモリ15をそれぞれユニット化して、耐タンパー容器に収めることにしておけば、適切な秘密の管理下で、情報Ａメモリ14と情報Ｂメモリ15を取り外して、新しい基地局１へ取り付ければよい。

【００４５】上記のように、本発明の第１の実施の形態では、暗号鍵バックアップ記憶装置を、秘密情報Ａを耐タンパー性の独立の情報Ａメモリに記憶し、秘密情報Ｂを耐タンパー性の独立の情報Ｂメモリに記憶し、秘密情報ＡとＢからバックアップ用暗号鍵を生成し、バックアップ用暗号鍵で通信暗号鍵を暗号化してバックアップファイルに格納し、暗号化された通信暗号鍵をバックアップ用暗号鍵で復号してリカバーする構成としたので、関係者や第三者に対して秘密を保持できる暗号鍵バックアップファイルを作成し、故障のときにはバックアップファイルより、安全かつ確実に暗号鍵をリカバーできる。

【００４６】（第２の実施の形態）本発明の第２の実施の形態は、３つの秘密情報をそれぞれ独立の耐タンパー性の秘密情報メモリに記憶し、３つの秘密情報の中の任意の２つの秘密情報から生成したバックアップ用暗号鍵で通信暗号鍵を暗号化してバックアップファイルに格納し、暗号化された通信暗号鍵をバックアップ用暗号鍵で復号してリカバーする暗号鍵バックアップ記憶装置である。

【００４７】図２は、本発明の第２の実施の形態における暗号鍵バックアップ記憶装置の機能ブロック図である。第１の実施の形態と異なるところは、情報Ａメモリ14と情報Ｂメモリ15に加えて、情報Ｃメモリ16を設けることにより、秘密情報を記憶するメモリの故障対策を行った点である。図２において、情報Ｃメモリ16は、図１に関して説明した情報Ａメモリ14と情報Ｂメモリ15と同じ特性を有するものである。また、情報Ｃメモリ16を設けることにより暗号計算部12の計算機能が変わる他は、各部の機能は第１の実施の形態と同じである。

【００４８】上記のように構成された本発明の第２の実施の形態における暗号鍵バックアップ記憶装置の機能と動作を説明する。最初に、情報Ａメモリ14、情報Ｂメモリ15、情報Ｃメモリ16に記憶する秘密情報の１例を説明する。情報Ａメモリ14に記憶する秘密情報をX1、情報Ｂメモリ15に記憶する情報をX2、情報Ｃメモリ16に記憶する秘密情報をX3とし、X1は、Sa、ｐ、ｎの３つのパラメータで構成し、X2は、Sb、ｑ、ｎの３つのパラメータで構成し、X3は、Sc、ｒ、ｎの３つのパラメータで構成する。ここで、ｐ、ｑ、ｒは、お互いに異なる十分に大きな素数とする。ｎは、十分に大きな整数で、１つの秘密

情報から暗号鍵を逆算することが困難な整数とする。Sa、Sb、Scは、

$Sa = K^p \bmod n$

$Sb = K^q \bmod n$

$Sc = K^r \bmod n$

とする。Kは、ＢＫ暗号鍵とする。これらの式の意味は、第１の実施の形態で説明した通りである。また、第１の実施の形態で説明した方法で、この秘密情報を生成し、記憶させることができる。

【００４９】秘密情報から暗号鍵Kを逆算して求めるときは、３つの秘密情報のうち、任意の２つの秘密情報を入手すれば、第１の実施の形態で述べた方法で、ＢＫ暗号鍵Ｋを求めることができる。すなわち、情報Ａメモリ14、情報Ｂメモリ15からSa、Sb、ｐ、ｑ、ｎを入手したとき、情報Ｂメモリ15、情報Ｃメモリ16からSb、Sc、ｑ、ｒ、ｎを入手したとき、情報Ｃメモリ16、情報Ａメモリ14からSc、Sa、ｒ、ｐ、ｎを入手したときのいずれも、暗号計算部12は暗号鍵Ｋを求めることができる。すなわち、整数ｐ、ｑ、ｒが互いに素であるとき、

$a1 \times p + b1 \times q = 1$

$a2 \times q + b2 \times r = 1$

$a3 \times r + b3 \times p = 1$

となる整数a1、b1、a2、b2、a3、b3が存在する。したがって、いずれの場合でも、第１の実施の形態で説明した計算方法でＢＫ暗号鍵Ｋを求めることができる。

【００５０】この計算方法によれば、情報Ａメモリ14、情報Ｂメモリ15、情報Ｃメモリ16のうち、任意の２つの秘密情報が得られれば、ＢＫ暗号鍵Kを求めることができる。すなわち、情報Ａメモリ14、情報Ｂメモリ15、情報Ｃメモリ16のうち、どれか１つが故障しても、残りの２つのメモリの情報からＢＫ暗号鍵Ｋを求めることができる。

【００５１】このアルゴリズムを利用すると、情報メモリを４つ以上設け、その中の２つの情報が得られれば、ＢＫ暗号鍵Kを求めるバックアップ装置装置を実現できる。すなわち、２台が故障から残れば、ＢＫ暗号鍵Kを求めることができる。

【００５２】本実施の形態を一般化すると、ｍ個の秘密情報を記憶するメモリを設け、その中のｔ個のメモリから秘密情報を得られれば、ＢＫ暗号鍵Kを求めることができる。これには、秘密分散と呼ばれる技術が適用できる。すなわち、しきい値がｔの秘密分散により、ＢＫ暗号鍵Kを秘密にすればよい。秘密分散によりＢＫ暗号鍵Kを求めることに必要な秘密情報の数を増やせば、それだけ不法にＢＫ暗号鍵Kを求めることが困難になる。ｔ＝ｍとすれば秘密保持性能は最大になるが、耐故障性は改善されない。ｔを小さくすれば耐故障性は向上するが、秘密保持性能は下がる。ｔをどのように選ぶかは、秘密保持性能と耐故障性との兼ね合いで決める。

【００５３】簡単な秘密分散の方式として、多元連立方程式を利用する方法がある。３元連立方程式を用いることで、秘密分散を５とし、しきい値を３とする。この場合、秘密情報１は、４つの整数パラメータX1、Y1、Z1、W1で構成し、秘密情報２は、４つの整数パラメータX2、Y2、Z2、W2で構成し、秘密情報３は、４つの整数パラメータX3、Y3、Z3、W3で構成し、秘密情報４は、４つの整数パラメータX4、Y4、Z4、W4で構成し、秘密情報５は、４つの整数パラメータX5、Y5、Z5、W5で構成する。

【００５４】W1、W2、W3、W4、W5は、以下の式

$aX1 + bY1 + cZ1 = W1$

$aX2 + bY2 + cZ2 = W2$

$aX3 + bY3 + cZ3 = W3$

$aX4 + bY4 + cZ4 = W4$

$aX5 + bY5 + cZ5 = W5$

を満足する値である。ａ、ｂ、ｃは秘密にしておきたい数（整数）である。上記、５式の中で、任意の３式のX、Y、Z、Wの数値が与えられれば、数値ａ、ｂ、ｃが求められる。この中の１つ、例えばａをＢＫ暗号鍵とするのである。

【００５５】具体的には、秘密情報の生成記憶過程では、暗号計算部12は、鍵生成器11で暗号鍵として、ａ、ｂ、ｃを発生させる。次に、乱数X1、Y1、Z1を発生し、ａ、ｂ、ｃとX1、Y1、Z1から計算でW1を求め、X1、Y1、Z1、W1の４つの数値を秘密情報１として、メモリに記憶させる。この計算を秘密情報の組数だけ繰り返す。最後に、ａ、ｂ、ｃを暗号計算部12から消去する。秘密情報の再生過程では、暗号計算部12は、３組の秘密情報をメモリから呼び出し、連立方程式を解いて、ａ、ｂ、ｃを求める。この例では、式を５つ用いたが、式の数はこれより多くてもよく、また、式の数が多いときでも多くの式の中から３つの式の情報をメモリから取り出せば、暗号鍵を求めることができる。

【００５６】信頼性について説明する。図２の装置では、暗号計算部12、鍵メモリ13、情報Ａメモリ14、情報Ｂメモリ15、情報Ｃメモリ16のどれか１つが故障しても、その部品を交換すれば、正常な装置に戻れる。すなわち、暗号計算部12、鍵メモリ13のどちらかが故障したときは、その部品を交換し、バックアップファイルからリカバーすれば正常に戻る。情報Ａメモリ14、情報Ｂメモリ15、情報Ｃメモリ16のどれかが故障したときは、その部品を交換し、バックアップ操作を行えば正常に戻る。

【００５７】このようにして、

（１）取り外し可能なバックアップファイルの媒体を入手しても、それだけでは、暗号鍵の秘密を解読できない。

（２）１個のメモリ部品が故障しても、バックアップファイルからリカバーできる。

（３）故障した秘密情報を記憶するメモリを１個入手し、解析しても、暗号鍵の秘密を解読できない。

という３つの条件を満足する装置が実現できる。

【００５８】上記のように、本発明の第２の実施の形態では、暗号鍵バックアップ記憶装置を、３つの秘密情報をそれぞれ独立の耐タンパー性のメモリに記憶し、３つの秘密情報の中の任意の２つの秘密情報からバックアップ用暗号鍵を生成し、バックアップ用暗号鍵で通信暗号鍵を暗号化してバックアップファイル手段に格納し、暗号化された通信暗号鍵をバックアップ用暗号鍵で復号してリカバーする構成としたので、秘密情報メモリの１つが故障しても、バックアップ用暗号鍵を生成して通信用暗号鍵をリカバーできる。

【００５９】（第３の実施の形態）本発明の第３の実施の形態は、通信用暗号鍵メモリと暗号計算部を一体に構成したモジュールと秘密情報メモリとの間を中継接続する耐タンパー性のモジュールを設け、秘密情報メモリと中継接続モジュールが非接続になったときに、秘密情報メモリの記憶内容を消去する暗号鍵バックアップ記憶装置である。

【００６０】図３は、本発明の第３の実施の形態における暗号鍵バックアップ記憶装置の機能ブロック図である。図３において、接続ユニット８は、暗号計算部12、情報Ａメモリ14、情報Ｂメモリ15、情報Ｃメモリ16を中継接続するもので、その代表的な形態は、マザーボードである。なお、図３では、情報Ａメモリ14の接続方法のみ詳細に図示している。図３において、情報メモリ14の接続部34のコネクターのプラグ／ソケットを別々に記載している。すなわち、接続部34pは、接続部34のプラグであり、接続部34sは、接続部34のソケットである。図１、図２に述べた暗号計算部12、情報Ｂメモリ15、情報Ｃメモリ16も、情報Ａメモリ14と同じ要領で接続ユニットと接続する。接続ユニット８は、電気的にアクセスすることが困難なモジュール、すなわち耐タンパー性のモジュールにする。電気的にアクセスすることを困難にするためには、接続ユニット８を樹脂で一体成形する。

【００６１】上記のように構成された本発明の第３の実施の形態における暗号鍵バックアップ記憶装置の機能と動作を説明する。図３に示す情報Ａメモリ14、情報Ｂメモリ15、情報Ｃメモリ16から暗号計算部12へ送るパスのうち、接続ユニット８では、樹脂一体成形などで耐タンパー性を向上させているため、電気的にアクセスすることが困難になっている。また、情報Ａメモリ14、情報Ｂメモリ15、情報Ｃメモリ16の耐タンパー性を向上させたものである。

【００６２】接続検出部Ｐ41p、接続検出部S41sは、秘密情報を渡すパス、すなわち接続部P34pと接続部Ｓ34sが接続されているかどうか、直接的または間接的に検出する。直接的に検出する方法としては、接続部34を経由して、電源を供給し、コネクターを外せば電源が消えることを原理とする方法がある。間接的検出方法としては、コネクターが外れたことを空間的に検出する原理による方法がある。

【００６３】図３に示す情報Ａメモリ14は、接続検出部Ｐ41pで、接続が切れたことを検出したときは、その信号を受けて、情報Ａメモリ14の記憶内容を消去する。耐タンパー性を向上させるためである。また、情報Ａメモリ14、情報Ｂメモリ15、情報Ｃメモリ16は、接続ユニット８から切り離した瞬間、接続検出部Ｐ41（情報Ｂメモリ15、情報Ｃメモリ16にも接続検出部Ｐ41と同じ機能を持たせるとしたとき）によって切り離しを検出し、情報Ａメモリ14、情報Ｂメモリ15、情報Ｃメモリ16の記憶内容を消去してしまうので、耐タンパー性が向上している。このようにして、情報Ａメモリ14から暗号計算部12へのパスを電気的にアクセスし難くするとともに、耐タンパー性を向上させる。

【００６４】上記のように、本発明の第３の実施の形態では、暗号鍵バックアップ記憶装置に、通信用暗号鍵メモリと暗号計算部を一体に構成したモジュールと秘密情報メモリとの間を中継接続する耐タンパー性のモジュールを設け、中継接続モジュールが非接続になったときに、秘密情報メモリの記憶内容を消去する構成としたので、秘密情報メモリを取り外して解読することができない。

【００６５】（第４の実施の形態）本発明の第４の実施の形態は、秘密情報を記憶した複数のメモリの中の一部を離れた場所に設置して伝送路を介して接続した暗号鍵バックアップ記憶装置である。

【００６６】図４は、本発明の第４の実施の形態における暗号鍵バックアップ記憶装置の機能ブロック図である。図４において、伝送装置Ａ51、伝送装置Ｂ52、伝送路53を除き、図１に示したものと同じである。伝送路53は、電話線などの有線伝送路、無線伝送路、ＬＡＮなどの伝送路であるが、単なる屋内配線であってもよい。伝送装置Ａ51、伝送装置Ｂ52は、情報Ｂメモリ15と接続部35の間の信号を伝送路の条件に合致する信号に変換／逆変換するものであり、伝送路53の種類に対応したものである。情報Ｂメモリ15は、伝送路を介して、基地局１から離れた場所に設置する。離れた場所とは、隣室であっても、隣りの建物でも、遠く離れた町でも、甚だしくは外国でもよい。

【００６７】上記のように構成した本発明の第４の実施の形態における暗号鍵バックアップ記憶装置の機能と動作を説明する。まず、鍵生成器で通信用暗号鍵を生成し、暗号計算部12を経由して鍵メモリ13へ書き込む。

【００６８】通信暗号鍵のバックアップファイルを作成するときは、鍵生成器で新しい暗号鍵１個をＢＫ暗号鍵として生成する。秘密情報を生成して、情報Ａメモリ14に書き込むとともに、伝送装置Ａ51を介して情報Ｂメモリ15にも書き込む。次に、暗号計算部12は、情報Ａメモリ14にある秘密情報を読み出すとともに、伝送装置Ａ51を介して情報Ｂメモリ15にある秘密情報を読み出し、Ｂ

Ｋ暗号鍵を求める。さらに、暗号計算部12は、鍵メモリ13に記憶している通信暗号鍵を、ＢＫ暗号鍵で暗号化して、ＢＫファイル18に書き込む。

【００６９】リカバリーを開始するとき、暗号計算部12は、情報Ａメモリ14にある秘密情報を読み出すとともに、伝送装置Ａ51を介して情報Ｂメモリ15にある秘密情報を読み出して、ＢＫ暗号鍵を求める。暗号計算部12は、暗号化されているバックアップ情報をＢＫファイル18から読み出してＢＫ暗号鍵で復号し、鍵メモリ13に書き込む。

【００７０】離れた場所に秘密情報を置くことにより、伝送路で盗聴される危険は増す（とはいっても、秘密情報を送るタイミングに盗聴しなくてはならないという盗聴の困難さがある）が、直接秘密情報を持ち出すことが難しくなる。特に、離れた場所に設置する効用が大きくなるケースとして、秘密分散のアルゴリズムにおいて、しきい値を増加すなわち秘密情報の数を増加し、増加した分を離れた場所に設置する場合がある。この場合、離れた場所の秘密情報が入手し難くなるという点で安全性が向上する。反面、増やした分の秘密情報が入手されても、増やす前に比べて安全性が低下することにはならない。本実施の形態では、秘密情報が２つの場合で説明したが、図２に示した秘密情報が３つ以上のケースでも適用できる。むしろ秘密情報が３つ以上のケースの方が、効用が大きい。

【００７１】上記のように、本発明の第４の実施の形態では、暗号鍵バックアップ記憶装置を、秘密情報を記憶した複数のメモリの中の一部を離れた場所に設置して伝送路を介して接続した構成としたので、秘密情報へのアクセスが困難になり、安全性が向上する。

【００７２】

【発明の効果】以上の説明から明らかなように、本発明では、暗号通信装置の暗号鍵バックアップ記憶装置を、通信に使う複数の通信暗号鍵を記憶する耐タンパー性の第１の記憶手段と、複数に分割した秘密情報をそれぞれ記憶する耐タンパー性の独立の複数の記憶手段からなる第２の記憶手段と、暗号計算手段と、バックアップファイル手段とを具備し、暗号計算手段は、第１の秘密情報と第２の秘密情報とに基づいてバックアップ用暗号鍵を生成する手段と、バックアップ用暗号鍵で複数の通信暗号鍵を暗号化してバックアップファイル手段に格納する手段と、暗号化された複数の通信暗号鍵をバックアップファイル手段から取り出してバックアップ用暗号鍵で復号して第１の記憶手段に格納する手段とを有する構成としたので、独立の複数の記憶手段の秘密情報とバックアップファイルを入手しないと暗号鍵を解読できなくなり、第三者のみならず従業員などの関係者にも暗号鍵の入手が困難になって、バックアップ／リカバリー過程における安全性を高めることができるという効果が得られる。

【００７３】また、暗号通信装置の暗号鍵バックアップ記憶装置を、通信に使う複数の通信暗号鍵を記憶する耐タンパー性の第１の記憶手段と、第１、第２、第３の秘密情報をそれぞれ記憶する耐タンパー性の独立の３つの記憶手段からなるである第２の記憶手段と、暗号計算手段と、バックアップファイル手段とを具備し、暗号計算手段は、第１の秘密情報と第２の秘密情報と第３の秘密情報の中の任意の２つの秘密情報に基づいてバックアップ用暗号鍵を生成する手段と、バックアップ用暗号鍵で複数の通信暗号鍵を暗号化してバックアップファイル手段に格納する手段と、暗号化された複数の通信暗号鍵をバックアップファイル手段から取り出してバックアップ用暗号鍵で復号して第１の記憶手段に格納する手段とを有する構成としたので、３つの秘密情報を記憶する記憶手段の１つが故障しても、２つの記憶手段の秘密情報からバックアップ用暗号鍵を生成してバックアップ／リカバリーができるという効果が得られる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態における暗号鍵バックアップ記憶装置の機能ブロック図、

【図２】本発明の第２の実施の形態における暗号鍵バックアップ記憶装置の機能ブロック図、

【図３】本発明の第３の実施の形態における暗号鍵バックアップ記憶装置の接続ユニットの機能ブロック図、

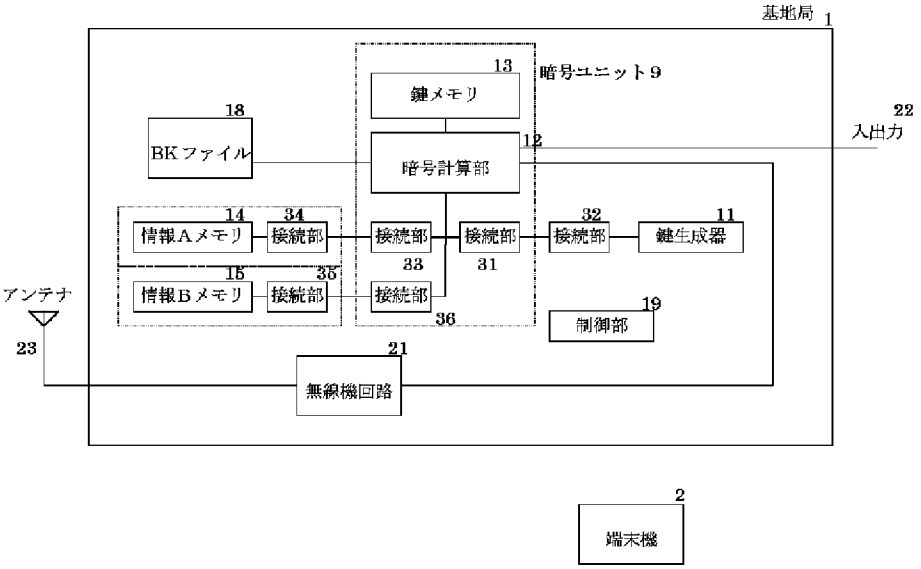
【図４】本発明の第４の実施の形態における暗号鍵バックアップ記憶装置の機能ブロック図である。

【符号の説明】

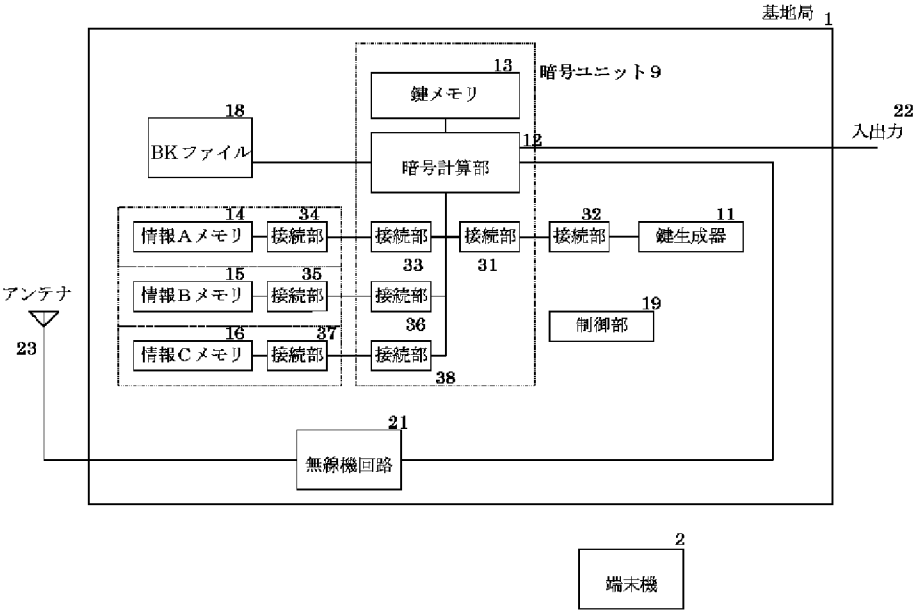
1　基地局
2　端末機
8　接続ユニット
9　暗号ユニット
11　暗号鍵生成器
12　暗号計算部
13　鍵メモリ
14　情報Ａメモリ
15　情報Ｂメモリ
16　情報Ｂメモリ
18　ＢＫファイル
19　制御部
21　無線機回路
22　入出力部
23　アンテナ
31　接続部
32　接続部
33　接続部
34　接続部
34p　接続部
34s　接続部
35　接続部
36　接続部

41p　接続検出部
41s　接続検出部
51　伝送装置
52　伝送装置
53　伝送路

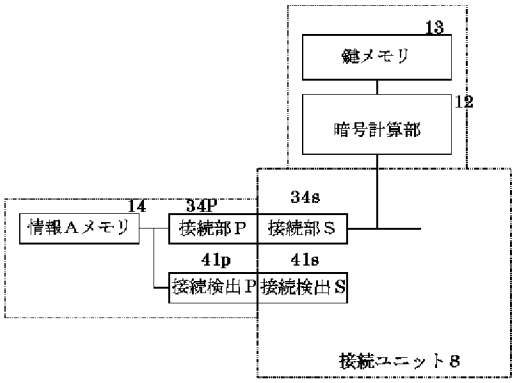
【図１】



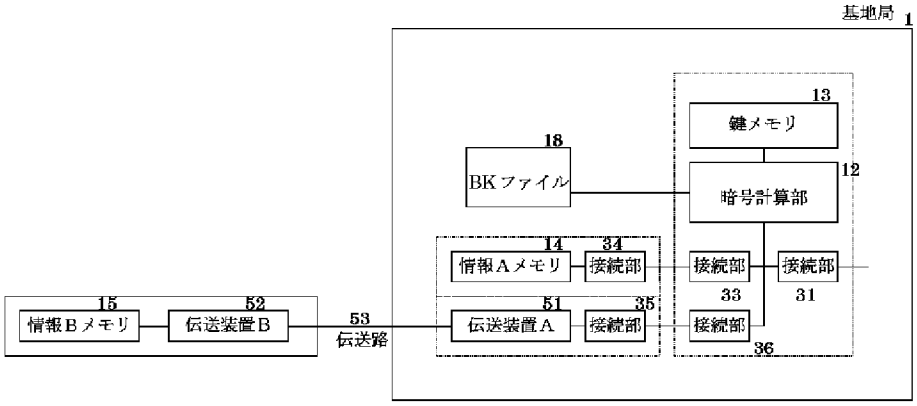
【図２】



【図３】



【図４】



フロントページの続き

Ｆターム(参考)　5B017 AA01 BA07 BB03 CA11 CA16
5B018 GA06 HA03 HA04 JA26 KA03
KA22 NA02 RA14
5J104 AA16 AA45 EA02 EA04 JA03
JA21 NA02 NA31 NA32 NA37
NA42 PA01